(12) UK Patent Application (19) GB (11) 2 362 543 (13) A

(43) Date of A Publication 21.11.2001

(21) Application No 0011608.7

(22) Date of Filing 16.05.2000

(51) INT CL[7]
H04Q 7/38

(52) UK CL (Edition S)
H4L LRCMS L205

(56) Documents Cited
GB 2342817 A EP 0336079 A2 WO 00/14895 A2

(58) Field of Search
UK CL (Edition S) H4L LRCMA LRCMS
INT CL[7] H04Q 7/32 7/38
Online: WPI, JAPIO, EPODOC

(71) Applicant(s)
Sagem SA
(Incorporated in France)
6 Avenue d'Iena, 75116 Paris, France

(72) Inventor(s)
Dan Duong

(74) Agent and/or Address for Service
W P Thompson & Co
Coopers Building, Church Street, LIVERPOOL, L1 3AB,
United Kingdom

(54) Abstract Title
Provision of a password to gain access to a computer network from a cellular telephone

(57) A security unit 11 of a mobile telephone 1 generates a password using an algorithm which is based upon on a secret code stored in the mobile and some other variable such as the current time and date. The algorithm may be as defined by the RADIUS protocol. The password and a user identifier are transmitted to a security server 4 by means of the access provider 3. The validity of the password and identifier are checked, and access to a computer network (such as the internet) is granted accordingly. A separate terminal 2, for example a portable computer, may be connected to the mobile for accessing the internet. The arrangement seeks to improve security by ensuring a different password is used each time a connection to a computer network is attempted.

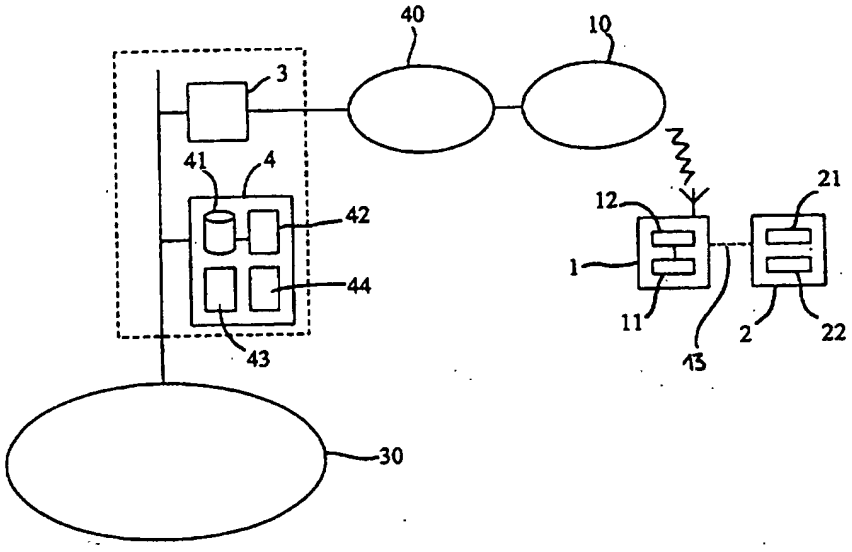

Figure 1

GB 2 362 543 A

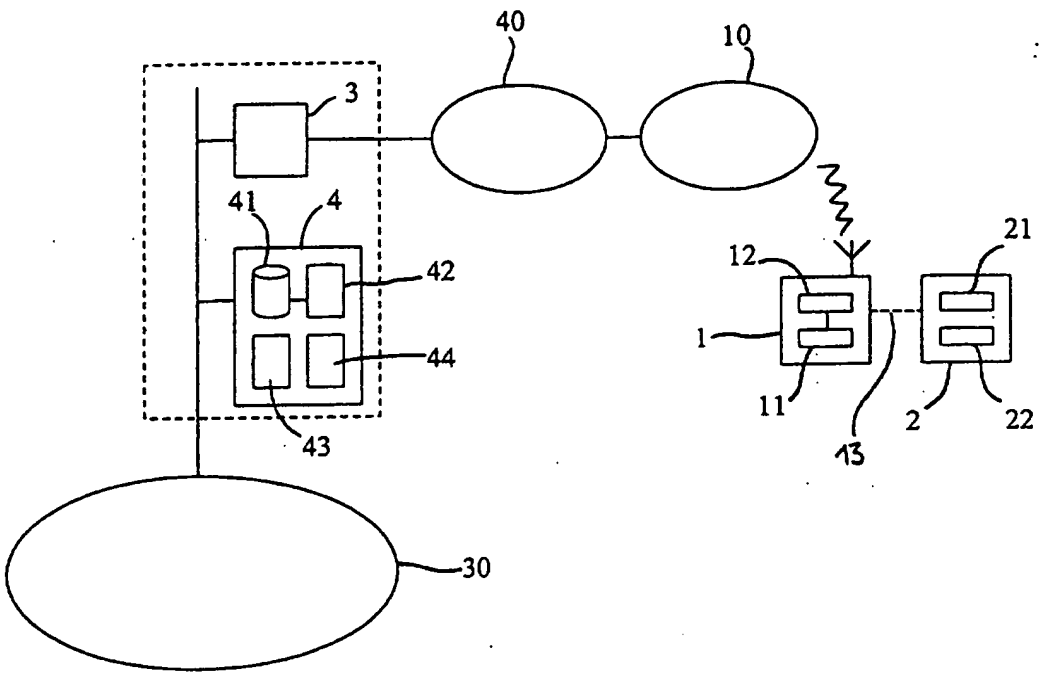

Figure 1

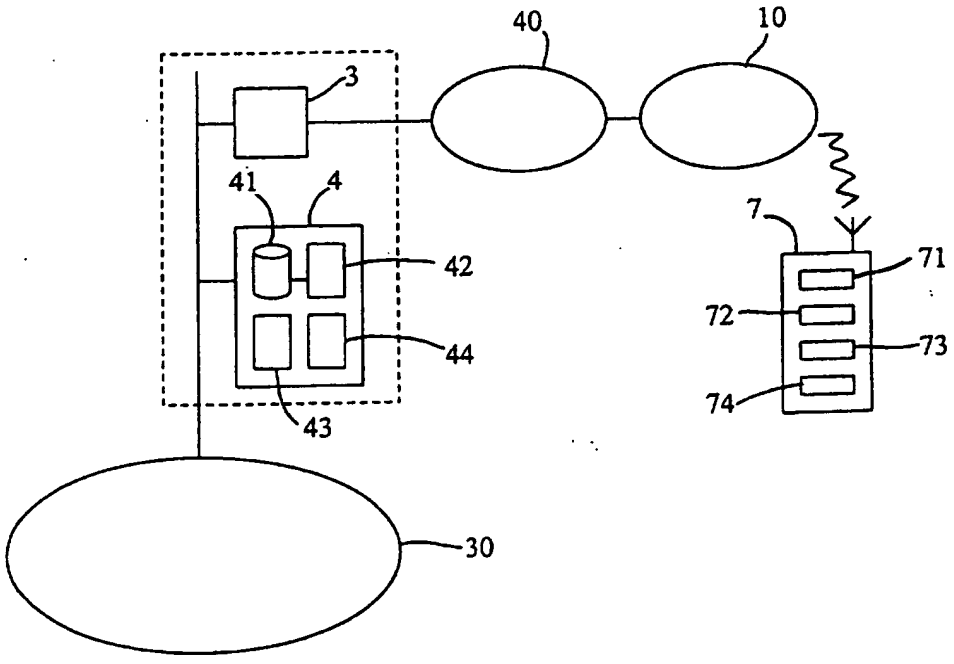

Figure 2

2362543

Description

Assembly of a cellular telephone and means for connection to a computer network

Some cellular telephones can be used to connect, to the Internet, a terminal, for example a portable computer provided with an Internet connection application. In operation, it is connected to the telephone, for example by a cable connection, the telephone connects the terminal to the Internet and, after connection, the terminal can navigate on the Internet, send or receive messages by means of the telephone. In this case, the telephone acts as a modem with respect to the terminal.

There are also cellular telephones having Internet capabilities permitting them to be connected to, and to communicate via, the Internet themselves.

In order to be connected to a computer network, for example the Internet, the equipment (terminal or telephone) must generally execute a protocol for telephone connection to an Internet access provider. This protocol comprises an authentication phase during which the equipment provides the access provider with an identifier and an associated user password. The access provider, in cooperation with a security server, identifies the equipment with the aid of its identifier and checks the validity of the password.

The password serves to make the Internet access secure. There are different levels of security. At level "0" the identifier is not associated with any password. At level "1" the password is fixed and immutable. At level "2" the password is dynamic and changes regularly.

In the case of a dynamic password, changing, for example upon each instance of connection to the Internet, the security server and the equipment must know the valid user password at the time of each connection.

To this end, the user can use a password "calculator" intended to generate passwords from at least one variable and a secret user code known to the security server, using an algorithm such as that defined by the RADIUS (Remote authentication dial-in user service) protocol, also implemented in the security server. The calculator and the security server are synchronised so that the security server recognises the valid user password generated by the calculator at the time of each connection.

When the user desires to connect his computer to the Internet by using his cellular telephone, he inputs his identifier into the terminal and activates his calculator by pressing an actuation key and inputs the telephone's PIN code. The calculator then generates a password from one or more variables, for example the date and time, and from the secret code and then displays this password. The user reads the password and inputs it manually into the terminal. The terminal then transmits the identifier and the user password to a security server via the cellular telephone and the Internet access provider. The security server determines the user password valid for this connection instance, associated with the identifier concerned, compares it with that provided by the terminal and, if they correspond, authorises Internet access.

The disadvantage of this mode of making Internet access secure resides in the fact that the user is obliged to carry with him not only the telephone but also

the calculator, which is cumbersome. Furthermore, the user may accidentally input an incorrect password into the telephone.

The present invention aims firstly to overcome this disadvantage.

To this end the invention relates to an assembly of a telephone of a cellular network and means for telephone connection to a computer network, which are intended, upon each instance of connection to the computer network, to provide a security server with an identifier and an associated password, wherein the telephone comprises security means arranged to generate different passwords upon different instances of connection to the computer network.

The invention thus consists of having integrated the calculator into the cellular telephone.

The Applicant has pointed out that the two operations carried out to activate the calculator (pressing an actuation key and inputting the PIN code) must also be carried out to actuate the cellular telephone. By integrating the calculator into the cellular telephone it will thus suffice to activate the telephone in order also to activate the security means. It is not necessary to input the PIN code manually twice.

The security means are advantageously arranged to provide, upon each instance of connection to the computer network, the connection means with a password which is valid for this connection.

Thus upon each connection instance, the password valid for this connection is transmitted to the connection means directly by the security means and not by the user. The user thus no longer has to input the password manually,

this password might no longer even be displayed.

It is also advantageous that means are provided to initialise the security means with the security server via the cellular network.

In the prior art it was necessary to bring the calculator to the security server, to connect them to each other, generally by an infrared connection, and to synchronise them in order to initialise the calculator. By means of the invention, the radio function of the telephone is used to initialise the security means remotely.

The security means are preferably arranged to generate a dynamic password from at least one variable and a secret code. The passwords can be generated from the date and time of connection and from a secret code stored in the telephone.

In one particular embodiment, the means for connection to the computer network are integrated into the telephone.

In another embodiment, the telephone comprises means for connection with a terminal comprising the said means for connection to the computer network.

The invention will be better understood with the aid of the following description, given by way of example only, of two embodiments of the assembly of the telephone and the means for connection to the computer network in accordance with the invention, with reference to the attached drawings in which:

- Figure 1 illustrates a functional block diagram of the assembly according to the first embodiment and

- Figure 2 illustrates a functional block diagram of the assembly according to the second embodiment.

The assembly of the invention illustrated in Figure 1 comprises a telephone 1 of a cellular network 10, in this case the GSM, and a unit 21 for connection to a computer network, in this case the Internet 30, integrated into a communication terminal 2, in this case a portable computer. The telephone 1 and the terminal 2 each comprise an infrared connector and a data interface to communicate with each other, permitting them to establish between them an infrared connection 13 for data transmission.

The terminal 2 has a means of access to the Internet 30 via a provider 3 of access to the Internet 30, and comprises the unit 21 for connection to the Internet 30 and an Internet navigator 22.

The access provider 3 is connected to a telephone network 40, in this case the STN and to a local computer network, also comprising a security server 4. Of course, the GSM telephone network 10 and STN 40 are interconnected. The access provider 3 and the security server 4 are connected to a central artery of the local network, which is itself connected to the Internet 30.

The Internet connection unit 21 comprises an application for connection to the Internet 30 permitting the terminal 2 to be connected to the access provider 3 via the cellular network 10 by executing a telephone connection protocol. This protocol comprises an authentication step during which the terminal 2 transmits an identifier and an associated user password to a security server 4 by means of the access provider 3. The security server 4 then checks the validity of these

identification data (identifier and password) in order to authorise or refuse access to the Internet 30 as will be explained hereinunder.

The Internet navigator 22 permits the terminal 2 to navigate on the Internet 30, in other words permits Web sites to be visited.

Apart from the standard elements of a cellular telephone, the telephone 1 comprises a security unit 11 intended to generate different passwords upon different instances of connection of the terminal 2 to the Internet 30, and a unit 12 for initialisation of the security unit 11. A PIN identification code allocated to the telephone 1 is stored in the memory of the telephone 1, not shown.

The security unit 11 is intended, upon each instance of connection to the Internet 30, to generate a password which is valid for this connection, and to supply this password to the connection unit 21 of the terminal 2 via the connection 13. The password, which is valid for one connection, is determined from two variables, in this case the date and time of the connection, and from a secret code stored in the telephone 1, by means of an algorithm which is defined in this case by the RADIUS protocol. The passwords are thus dynamic, ie. they are not fixed and change upon each instance of connection to the Internet 30.

The initialisation unit 12 is arranged to initialise the security unit 11 under the control of the user. The initialisation consists of synchronising the security unit 11 and the security server 4 so that each time the terminal 2 is connected to the Internet 30, the server 4 recognises the password which is valid for this connection, generated by the telephone 1 as explained hereinunder.

The security server 4 is intended to control access to the Internet 30 of a

number of pieces of user equipment comprising in particular the terminal 2. It comprises a database 41 of users, a unit 42 for managing the database 41, a security unit 43 and an access control unit 44.

The database 41 of users contains, for each user, an identifier and possibly an associated secret code. The base 41 contains, in particular the identifier of a user of the terminal 2.

The security unit 43 is intended, upon each instance of connection of a piece of user equipment, to determine the password valid for this connection by implementing the same password-generation algorithm as that implemented in the telephone 1.

The access control unit 44 in cooperation with the security unit 43 is intended, upon each instance of connection of a piece of user equipment, to check the validity of the identifier and of the associated user password, which are provided by this piece of equipment.

Before the terminal 2 is connected to the Internet 30 for the first time, the security unit 11 should be initialised, in other words it should be synchronised with the security server 4. To do so the user inputs an initialisation command by selection in GUI (Graphical User Interface) menus of the telephone 1, thus activating the initialisation unit 12. The following steps of initialisation of the security unit 11 are executed automatically under the control of the initialisation unit 12.

By means of its GUI, the telephone 1 invites the user to input his identifier which is known to the security server 4, and a secret code which is not yet known

to the security server 4, from which the connection passwords will be generated. Using the keypad of the telephone 1, the user then inputs his identifier and the secret code. The secret code is then stored, in this case in the telephone 1, for subsequent connections to the Internet 30.

The telephone 1 then calls the access provider 3 via the cellular network 10, establishes telephone communication therewith and then sends an initialisation request containing the identifier and the secret user code, which are input by the user, to the security server 4 via the access provider 3.

Upon receipt of this request the security server 4 looks for the identifier in the database 41 and stores the secret user code therein, associating it with this identifier.

The operation of connecting the terminal 2 to the Internet 30 will now be described.

In order to connect the terminal 2 to the Internet 30, a user actuates the telephone 1 by pressing an actuation key and then inputting the PIN code of the telephone 1, and actuates the terminal 2. The user then connects the telephone 1 and the terminal 2 by an infrared connection and instigates the application (21) for connection to the Internet 30 on the terminal 2. The user then inputs his identifier into the terminal 2 and orders connection of the terminal 2 to the Internet 30.

The terminal 2 then transmits to the telephone 1, a telephone call command of the access provider 3, containing the telephone call number thereof, with an indication specifying that it is a call for connection to the Internet 30.

The telephone 1 then calls the access provider 3 via the cellular network

10 and establishes telephone communication therewith.

Upon receipt of the indication specifying that the call is a call for connection to the Internet 30, the security unit 11 of the telephone 1 generates a password which is valid for the connection, from the current date and time and from the secret user code stored in the telephone 1, and supplies this password to the connection unit 21 of the terminal 2.

After establishing the telephone communication between the telephone 1 and the access provider 3, the terminal 2 executes a protocol for telephone connection with the access provider 3 by means of the telephone 1. This protocol comprises an authentication phase during which the terminal 2 transmits to the security server 4, by means of the access provider 3, the user identifier and the password generated by the telephone 1.

Upon reception of the identifier and of the associated password, the security server 4 looks for the identifier in the database 41, extracts therefrom the associated secret code, determines the password valid for this connection instance from the date, time and secret code, compares this password with that received and, if they correspond, enables the connection to the Internet 30.

In the description above, the telephone 1 and the terminal 2 are connected by an infrared connection. They could also be connected by any other type of wireless connection ("bluetooth", DECT, etc) or by a cable connection.

The second embodiment of the invention differs from the embodiment just described only in the ways now to be explained.

The telephone 7 illustrated in Figure 2 is a telephone of the cellular

network GSM 10, having means of access to the Internet 30 via the access provider 3. A PIN identification code is allocated to the telephone 7 and stored in a memory thereof, not shown.

Apart from the standard elements of a cellular telephone, the telephone 7 comprises a unit 71 for connection to the Internet 30, an Internet navigator 72, a security unit 73 and a unit 74 for initialisation of the security unit 73.

The Internet connection unit 71 permits the telephone 7 to be connected to the Internet 30 via the cellular network 10 by means of the provider 3 of access to the Internet 30 by executing a telephone connection protocol. This protocol comprises an authentication phase during which the telephone 7 provides the security server 4 with an identifier and an associated user password via the access provider 3.

The security unit 73 is intended, each time the telephone 7 is connected to the Internet 30, to generate a password which is valid for this connection and to supply this password to the connection unit 71. The password, which is valid for one connection instance, is determined from the current date and time and from a secret code, which is in this case stored in the telephone 7, with the aid of the algorithm defined by the RADIUS protocol.

The initialisation unit 74 is intended to initialise the security unit 73, in other words, to synchronise the security unit 73 and the security server 4 so that, each time the telephone 7 is connected to the Internet 30, the server 4 recognises the password which is valid for this connection instance and is generated by the telephone 7.

Before the terminal 7 is connected to the Internet 30 for the first time, the security unit 73 should be initialised. In order to do so, the user activates an initialisation command by selection in the GUI menus of the telephone 7. The following initialisation steps of the security unit 73 are then executed automatically under the control of the initialisation unit 74.

Upon invitation of the telephone 7, the user then inputs his identifier which is known to the security server 4, and a secret code which is not yet known to the security server 4, with the aid of the keypad of the telephone 7. The secret code is stored in the telephone 7 for subsequent instances of connection to the Internet 30. The telephone 7 then calls the access provider 3 via the cellular network 10 and, after establishing the telephone communication, sends the security server 4, by means of the access provider 3, an initialisation request containing the identifier and the secret user code which have been input. Upon receipt of this request the security server 4 looks for the identifier in the database 41 and stores therein the secret user code, associating it with this identifier.

The operation of connecting the terminal 2 to the Internet 30 will now be described.

After having actuated the telephone 7 by pressing an actuation key and inputting the PIN code, a user activates a command for connection to the Internet 30, in this case by pressing a specific Internet key, and inputs its identifier with the aid of the keypad of the telephone 7.

Upon activation of the command for connection to the Internet 30, the telephone 7 automatically executes the steps described hereinunder for connection

to the Internet 30.

Under the control of the Internet connection unit 71, the telephone 7 calls the provider 3 of access to the Internet 30 via the cellular network 10 and establishes telephone communication therewith.

Furthermore, the security unit 73 generates a password which is valid for the current connection instance, and supplies it to the connection unit 71.

After establishing communication between the access provider 3 and the telephone 7, the telephone 7 executes the protocol for telephone connection to the Internet 30 under the control of the connection unit 71. During the authentication phase of this protocol, the telephone 7 transmits the user identifier and the password which is valid for this connection instance to the security server 4 by means of the access provider 3.

Upon receipt of the identifier and of the associated password, the security server 4 looks for the identifier in the database 41, extracts therefrom the associated secret code, determines the password valid for this connection instance from the date, time and secret code, compares this password with that received and, if they correspond, enables the connection to the Internet 30.

In the description above, the user of the terminal 2 or of the telephone 7 inputs his identifier upon each instance of connection to the Internet 30. As an alternative, he could input his identifier upon connection to the Internet 30 and store it for the following connection instances.

It is emphasised that the password which is generated by the telephone 1 or 7 upon each instance of connection to the Internet 30 is not displayed but is

supplied directly to the Internet connection unit integrated into the telephone 7 or into the terminal 2.

It will also be noted that the initialisation of the security unit 11 (73) of the telephone 1 (7) with the security server 4 is carried out remotely via the cellular network 10 by using the radio telephony function of the telephone 1 (7).

The password could be formed from one or more variables other than the date and time and from a secret code. The variable could be, for example a number which is incremented each time the terminal 2, or the telephone 7, is connected to the Internet 30.

Instead of generating a different password upon each instance of connection to the Internet 30, the security unit of the terminal 2, or of the telephone 7, could generate a different password every "x" connection instances, "x" being fixed or variable.

In the description above, during initialisation of the security unit of the telephone, the user inputs a secret code which is then stored in the telephone.

In one variation, this secret code could be input by the user upon each instance of connection to the Internet.

In another variation, the secret code could be stored in the telephone during manufacture. In this case the secret code could be stored in the security server with the associated user identifier without any intervention of the telephone.

Instead of being separate, the security server 4 and the server 3 providing access to the Internet 30 could be integrated into a single server.

The terminal 2 and the telephone 7 could comprise an electronic Internet messaging application.

The invention could be applied to any computer network other than the Internet.

CLAIMS

1. An assembly of a telephone of a cellular network and means for telephone connection to a computer network, which are intended, upon each instance of connection to the computer network, to provide a security server with an identifier and an associated password, wherein the telephone comprises security means arranged to generate different passwords upon different instances of connection to the computer network.

2. An assembly according to claim 1, wherein the security means are arranged to provide, upon each instance of connection to the computer network, the connection means with a password which is valid for this connection instance.

3. An assembly according to any of claims 1 and 2, wherein means are provided to initialise the security means with the security server via the cellular network.

4. An assembly according to any of claims 1 to 3, wherein the security means are arranged to generate the passwords from at least one variable and a secret code.

5. An assembly according to claim 4, wherein the security means are arranged in order, upon each instance of connection to the computer network, to generate a password from the date and time of the connection and from a secret code stored in the telephone.

6. An assembly according to any of claims 1 to 5, wherein the means for connection to the computer network are integrated into the telephone.

7. An assembly according to any of claims 1 to 5, wherein the telephone

comprises means for connection to a terminal comprising the said means for connection to the computer network.

8. An assembly substantially as herein described, with reference to, and as illustrated in, the accompanying drawings.

Amendments to the claims have been filed as follows

CLAIMS

1. An assembly of a telephone of a cellular network and means for telephone connection to a computer network, which are intended, upon each instance of connection to the computer network, to provide a security server with an identifier and an associated password, wherein the telephone comprises security means arranged to generate different passwords from at least one variable and a secret code upon different instances of connection to the computer network.

2. An assembly according to claim 1, wherein the security means are arranged to provide, upon each instance of connection to the computer network, the connection means with a password which is valid for this connection instance.

3. An assembly according to any of claims 1 and 2, wherein means are provided to initialise the security means with the security server via the cellular network.

4. An assembly according to claim 1, wherein the security means are arranged in order, upon each instance of connection to the computer network, to generate a password from the date and time of the connection and from a secret code stored in the telephone.

5. An assembly according to any of claims 1 to 4, wherein the means for connection to the computer network are integrated into the telephone.

6. An assembly according to any of claims 1 to 4, wherein the telephone comprises means for connection to a terminal comprising the said means for connection to the computer network.

7. An assembly substantially as herein described, with reference to, and as illustrated in, the accompanying drawings.

The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

Application No:	GB 0011608.7	**Examiner:**	Glyn Hughes
Claims searched:	1 to 8	**Date of search:**	5 January 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4L (LRCMS, LRCMA)

Int Cl (Ed.7): H04Q 7/32, 7/38

Other: Online: WPI, JAPIO, EPODOC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
Y	GB 2342817 A	(NOKIA) see page 11 line 19 to page 13 to line 29	1-3, 6, 7
Y	EP 0336079 A2	(MOTOROLA) see figure 2 and column 7 line 16 to column 9 line 16	1-3, 6, 7
Y	WO 00/14895 A2	(DETEMOBIL) see abstract	1 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.